

## Chapter 6

---

# Performing server backups

### In this chapter

|                                                                     |     |
|---------------------------------------------------------------------|-----|
| <u>Overview</u>                                                     | 142 |
| <u>Section A: About performing server backups</u>                   | 143 |
| <u>About backing up server data</u>                                 | 144 |
| <u>Section B: Working with backup devices</u>                       | 149 |
| <u>About backup devices</u>                                         | 150 |
| <u>Adding backup devices to the Backup Devices window</u>           | 154 |
| <u>Modifying or deleting backup devices</u>                         | 156 |
| <u>Section C: Scheduling server backups</u>                         | 159 |
| <u>About scheduling server backups</u>                              | 160 |
| <u>Opening the Backup Scheduler</u>                                 | 163 |
| <u>Scheduling server backups</u>                                    | 165 |
| <u>Modifying and deleting scheduled backups</u>                     | 170 |
| <u>Monitoring or canceling backups</u>                              | 171 |
| <u>Section D: Setting up remote disk backups</u>                    | 175 |
| <u>About remote disk backups</u>                                    | 176 |
| <u>Planning the configuration</u>                                   | 177 |
| <u>Creating a writable share on the remote file server</u>          | 179 |
| <u>Reconfiguring the backup and restore on the CallPilot server</u> | 199 |
| <u>Verifying the network configuration</u>                          | 204 |
| <u>Creating a disk device on the CallPilot server</u>               | 206 |
| <u>Section E: Restoring your CallPilot system</u>                   | 207 |
| <u>Restoring your CallPilot system from the base hardware</u>       | 208 |

## Overview

### Introduction

This chapter provides information on how to schedule server backups to prevent data loss, and how to restore the CallPilot server after a failure.

- Section A: “About performing server backups,” on page 143, describes the types of predefined backups that are available.
- Section B: “Working with backup devices,” on page 149, describes the backup devices that are provided and recommended, and how to define new backup devices.
- Section C: “Scheduling server backups,” on page 159, describes how to schedule a predefined backup. It also provides information on how to modify or delete a scheduled entry, and how to monitor or cancel a running backup.
- Section D: “Setting up remote disk backups,” on page 175, describes how backups can be performed to a remote disk.
- Section E: “Restoring your CallPilot system,” on page 207, describes how to locate the procedures for restoring the CallPilot server from the base hardware.

## **Section A: About performing server backups**

### **In this section**

About backing up server data

144

## About backing up server data

### Introduction

A server backup lets you save and restore a complete set of system and multimedia data files from your CallPilot server in the event of disk drive failure or corrupted or lost configuration and messaging data. Backups also protect against data loss due to theft or damage caused by natural disasters.

A complete server backup consists of a single backup for each logical disk drive installed on your server. If you want to do a specific backup of user archives, prompt archives, or Application Builder archives, see [Chapter 7, “Archiving and restoring data from archives.”](#)

You can back up files to server tape or to another specified device. Backups are scheduled from the CallPilot Administration Client. They can also be performed immediately using the Tool Launcher on the server.

Perform server backups frequently and at regular intervals to prevent data loss.

### Restoring from backups

#### ATTENTION

Your distributor is responsible for restoring server backups to return the server to the state it was in when the backup was created.

Procedures for reinstalling the CallPilot system and restoring your data are located in Part 5 of the *Installation and Configuration Guide* for your platform.

### RAID systems

Backups protect against data loss due to software problems (for example, file system corruption, registry corruption, and failed upgrades), undetected disk errors, double faults, and human error. In addition, backups are useful for migration to a different CallPilot platform. For these reasons, Nortel Networks recommends that periodic backups be done even on servers with RAID. Store the backup tapes separately from the CallPilot server.



## Required security level and password

### Security

Log on to the CallPilot Administration Client with an administrator user ID.

### Password

The CallPilot Backup and Restore service requires the same password as the password used for NGenSys.

If you have changed the Windows NT user account password for NGenSys, see "To change the CallPilot Backup and Restore service password to match NGenSys" on page 426.

## Requirements

To perform a complete server backup, schedule predefined backups to correspond to the number of drives on your server. Before you schedule a predefined backup, ensure that the destination device is listed in the Backup Devices table.

## Predefined server backups

When you install CallPilot, two types of predefined server backups are installed on the server—the system backup and the secondary disk backup. These backups are not scheduled to run automatically. You must schedule them using the Backup Scheduler.

To schedule a predefined backup, see Section C: "Scheduling server backups," on page 159.

A complete set of server backups consists of

- a system backup
- one secondary disk backup for each additional disk drive on your server (for example E, F)

You can schedule the backups separately; however, you must have a backup of all disks to do a complete restore of the CallPilot server.

**System backup**

The system backup saves all your data on drives C and D. Schedule a system backup to copy the following items to the specified backup device:

- the database
- Windows NT registry
- Multimedia File System (MMFS) volume 1
- Nortel Networks dynamic data files

**Secondary disk backups**

The secondary disk backup saves all your data stored on the additional disks on the server. Each disk represents one volume.

**Note:** On a RAID system, you back up a partition on a mirrored disk pair where two disks represent one volume. For example, if you have four disks, they equal two volumes; therefore, you do two secondary disk backups for the two volumes.

Schedule secondary disk backups to copy the following items to the specified backup device:

- recorded user messages
- greetings
- customized prompts
- Application Builder prompts and applications

**Excluded data**

Server backups do not save the following software. If a catastrophic failure occurs, you must reinstall this software as part of the complete CallPilot system restore procedure:

- Windows NT 4.0
- CallPilot server software
- CallPilot client software
- Any PEPs applicable to your system

The *Installation and Configuration Guide* for your server describes the complete restore procedures. Your distributor is responsible for data restore procedures from backup for your system.

## Backup speed

The speed with which backups are performed depends on the current load on the system and whether the backup device is local.

The following table illustrates the total elapsed time required to perform a backup for various system types and sizes. The Total Backup Elapsed Time (in minutes) includes the time to back up system and user data. For example, the time to back up a 200i system with a 4 Gbyte tape drive, no load, 30 hours of user data, and the system data is 29 minutes.

| Total Backup Elapsed Time (in minutes) |                                             |            |             |             |             |              |
|----------------------------------------|---------------------------------------------|------------|-------------|-------------|-------------|--------------|
| Platform                               |                                             | 30<br>hour | 100<br>hour | 200<br>hour | 600<br>hour | 1000<br>hour |
| <b>200i</b>                            | 4 Gbyte tape drive, no load                 | 29         | 60          | 103         |             |              |
|                                        | 4 Gbyte tape drive, with 100% channels busy | 40         | 71          | 114         |             |              |
| <b>702t</b>                            | 16 Gbyte tape drive, no load                | 11         | 18          | 28          | 69          | 110          |
|                                        | 16 Gbyte tape drive, 75% channels busy      | 16         | 23          | 33          | 74          | 115          |
| <b>1001rp</b>                          | 16 Gbyte tape drive, no load                | 11         | 18          | 28          | 69          | 110          |
|                                        | 16 Gbyte tape drive, 75% channels busy      | 16         | 23          | 33          | 74          | 115          |

Restore times are comparable to no-load backup times.

## Formulating a backup strategy

A well-planned backup strategy minimizes the risk of losing data. When you formulate your strategy, consider the following points:

- Which data is critical to the organization and should be backed up?
- How often does data change?  
Periodically, you can back up data that changes infrequently. Back up data that changes constantly more often, especially if it is critical to the organization.
- Who will maintain the backups and do they fully understand their roles? Be sure they know how to label backup media for easy retrieval.
- Determine on-site and off-site locations for backup media. Ensure that only authorized personnel have full access to the sites. Store your backup media in an environment that meets the media manufacturer's storage requirements.

## Section B: Working with backup devices

### In this section

|                                                           |            |
|-----------------------------------------------------------|------------|
| <u>About backup devices</u>                               | <u>150</u> |
| <u>Adding backup devices to the Backup Devices window</u> | <u>154</u> |
| <u>Modifying or deleting backup devices</u>               | <u>156</u> |

## About backup devices

### Introduction

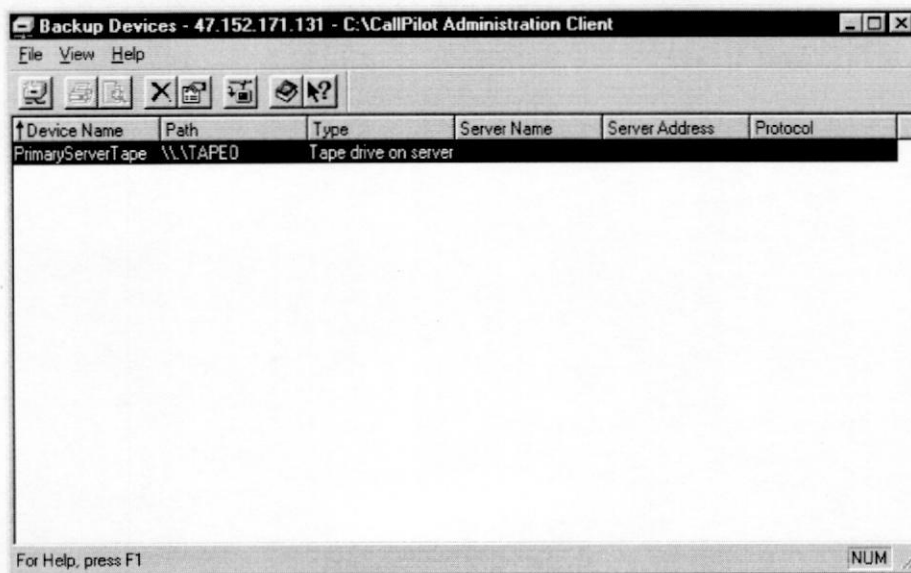
When you schedule a predefined backup, you must specify a destination backup device that is listed in the Backup Devices window.

Some devices are predefined and automatically listed in the Backup Devices window when the CallPilot server software is installed. If the device for the backup that you want to schedule is not listed, add it to the Backup Devices window.

**Getting there** CallPilot System > System Administration > Server Backup > Backup Devices

### The Backup Devices window

The Backup Devices window lists all destination devices for which you can schedule a backup.





To add a backup device to the Backup Devices window, see [“Adding backup devices to the Backup Devices window”](#) on page 154.

## Predefined devices

The following devices are predefined by the server software. These devices automatically appear in the Backup Devices window if the server is configured to list them.

**Note:** The PrimaryServerDisk device is no longer available as a backup device. The PrimaryServerDisk represents local disk space that must not be used for server backups because the backed-up data is lost if the disk fails.

### PrimaryServerTape

The PrimaryServerTape represents a tape drive located on the server. The PrimaryServerTape is the most common device for backups.

The PrimaryServerTape is always listed in the Backup Devices window. Before scheduling a backup to the PrimaryServerTape, make sure that a tape drive is installed on your CallPilot server.

### ATTENTION

Do not change the directory path to the backup device. Changing the path will cause the backup to fail.

### Remote disk backups

You can configure the CallPilot server to allow backups to be performed to a remote file server, such as a Windows 95/98 workstation or Windows NT server, rather than a tape drive.

For more information on setting up remote disk backups, see [“About remote disk backups”](#) on page 176.

## Tape devices

All backup tapes must be specially formatted for server data. When you schedule a backup, you can select Autoformat to format the tape, if necessary, immediately before the scheduled backup runs. This process destroys existing data on the tape.

**Overwriting existing data**

When you schedule a backup, select Overwrite to replace the contents of the tape with the new backup. If you do not select Overwrite, the new backup is appended to existing server backup data on the tape.

**Note:** If you schedule your system backup and your secondary disk backups to run one after the other and intend to use the same tape, select Overwrite only on the first backup. If you select Overwrite on the subsequent backups, you overwrite the data from the earlier one.

**Recommended devices**

You can perform backups on remote hard disks, or with the following tape drives:

- Tandberg SLR32 QIC
- Tandberg SLR5
- Tandberg SLR50
- MLR1

**Verify that backups are successful**

Nortel Networks recommends that you periodically verify that your scheduled backups are completed successfully, with no items skipped. Skipped items on server backups indicate a problem—such backups might not provide sufficient data to restore your system completely in the event of a catastrophic failure.

You can determine the completion status of your most recent backups using the Event Browser on the Administrative Client (see “Using the Event Browser” on page 271). You can filter on event codes 41800 through 41899 to view all recent initiations and completions of backups and restores, as well as other significant backup/restore events.

To see a more extensive history of backup completion status, open the Backup Scheduler on the Administrative Client. This dialog box automatically pops up a scrollable dialog box showing the completion status of all backups performed in the last 90 days. See “Opening the Backup Scheduler” on page 163 for details.

A detailed diagnostic log for each backup completed in the last 90 days is available in the server directory D:\Nortel\Data\Backup\BackupLogs. The logfiles are named for the backup that was done (for example, *SystemBackup*, followed by the date and time the backup was started, with the file extension *log*).

**Note:** Some messages in this diagnostic log, which appear to be error messages, are in fact normal events that are handled by the Backup/Restore service, and do not necessarily indicate a problem. Your primary indication of backup problems is that the overall completion status is other than *successful* with no items skipped.

### Storage and maintenance

Rotate backup tapes regularly and store at least one set of server backups off-site. Do not keep a tape in the tape drive for an extended period of time for the following reasons:

- If the same tape is used for several consecutive backups and the tape becomes damaged, no other backup is available to restore lost data.
- Consistent reuse of the same tape accelerates wear on the tape. You might need to replace tapes earlier than their normal life span.

To prolong the life of your tape heads and ensure the quality of backups, purchase and use head-cleaning kits. Clean tape drives based on the frequency of use. Recommended guidelines for cleaning are provided with most cleaning kits.

## Adding backup devices to the Backup Devices window

### Introduction

You can only schedule a backup on those devices listed in the Backup Devices window. If the device is not listed, add it to the window before you schedule a backup.

### Predefined devices

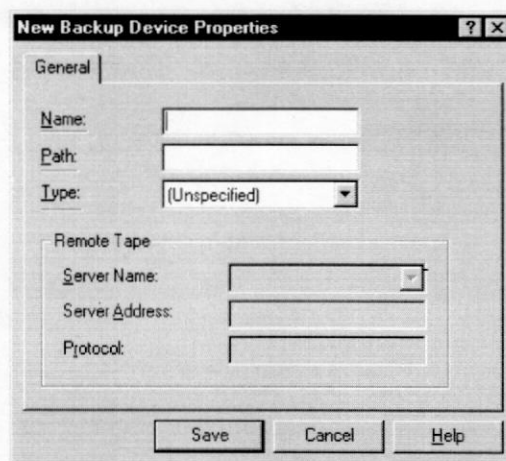
When the CallPilot server is installed, predefined devices are listed. For more information on these devices, see [“About backup devices” on page 150](#).

**Getting there** CallPilot System > System Administration > Server Backup > Backup Devices

### To add a backup device

- 1 In the Backup Devices window, click File > New.

**Result:** The New Backup Device Properties window appears.



- 2 Specify a name for the device.

**Note:** The limit is 240 characters.

- 3 Based on whether the device is local or remote disk space, enter the path of a disk directory as follows:

- For local disk directories, enter the absolute pathname (for example, E:\TEMP).

**ATTENTION**

---

If you define a local disk device, do not use it for server backups. A local disk device does not provide adequate protection against disasters. Also, the local disk device can quickly become full and might cause unrecoverable data corruption.

- For remote disk directories, enter the universal naming convention path (for example, \\SERVER1\BACKUPDATA).

- 4 Specify the type of backup device.
- 5 Click Save.



## Modifying or deleting backup devices

### Introduction

This section describes how to

- modify a backup device
- view details about a backup device
- delete a backup device from the Backup Devices window

**Getting there** CallPilot System > System Administration > Server Backup > Backup Devices

### To modify a backup device

- 1 In the Backup Devices window, click File > Properties.

**Result:** The Backup Device Properties window appears.



- 2 Modify any of the following fields:

- Name
- Path
- Type

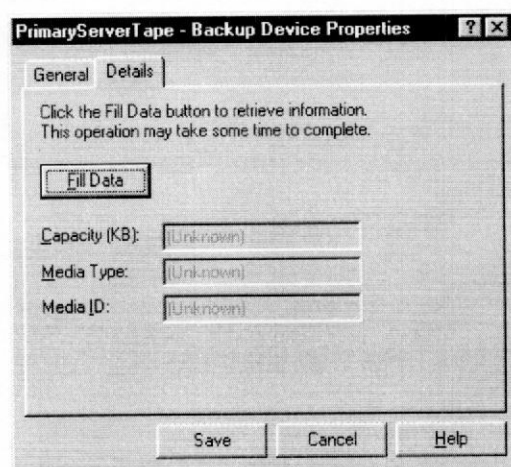


- 3 Select Save to save changes to the Backup Device properties.

### To view details for a backup device

- 1 In the Backup Devices window, click File > Properties.  
**Result:** The Backup Device Properties window appears.
- 2 Click the Details tab.

**Result:** The Details page appears.



### To delete a backup device

- 1 In the Backup Devices window, select the backup device that you want to delete.
- 2 Click X in the Backup Devices window toolbar.



## Section C: Scheduling server backups

### In this section

|                                                 |            |
|-------------------------------------------------|------------|
| <u>About scheduling server backups</u>          | <u>160</u> |
| <u>Opening the Backup Scheduler</u>             | <u>163</u> |
| <u>Scheduling server backups</u>                | <u>165</u> |
| <u>Modifying and deleting scheduled backups</u> | <u>170</u> |
| <u>Monitoring or canceling backups</u>          | <u>171</u> |

## About scheduling server backups

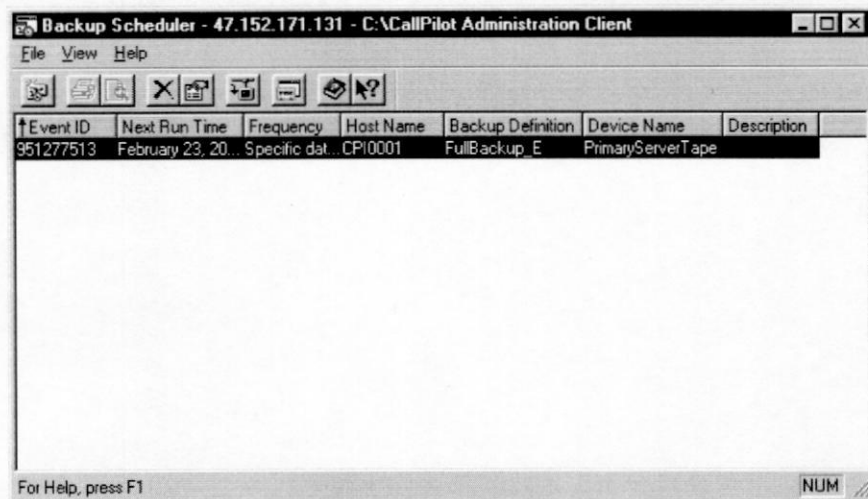
### Introduction

After the CallPilot server is installed and operational, schedule the appropriate server backups to run using the Backup Scheduler.

Log on to the CallPilot Administration Client as an administrator.

### The Backup Scheduler

When you schedule a backup, it appears in the Backup Scheduler.



### When backups should run

Schedule backups to run at the following times:

- before and after major system operations take place, such as an upgrade or the application of PEPs
- after you make any major modifications, such as the addition of a large number of users or customized prompts

- at regular intervals during normal operation, according to the criticality of your message data

Even though running a backup at peak hours has only a minimal impact on response time, try to run backups at off-peak hours whenever possible.

**Note:** If you do administrative tasks while a backup is in progress, that work might be lost if the backup is used to do a restore.

## What scheduling involves

To schedule a backup, open the Backup Scheduler to gain access to the Event Properties window. In this window, name the backup and select the destination device and the type of backup. You must also do the following steps:

### Specify the dates and times of the backup

Schedule a backup to run once on a specific day and time, or at regular intervals (daily, weekly, monthly, yearly).

### Specify a maximum wait interval (optional)

The maximum wait interval is the period of time during which a scheduled backup attempts to run if it cannot start on time. Specify the maximum wait interval to reduce the risk of missing a backup due to conflicts between the backup and other events, such as the MMFS audit.

#### Notes:

- Set the maximum wait interval so that if the backup must wait the maximum time, it still completes within the off-peak period.
- If a backup cannot start at the specified time, an Information Event is generated. If the backup cannot start within the specified maximum wait interval, a minor alarm is generated. See Part 2, "Monitoring the CallPilot system," for information on how to interpret alarms.

#### ATTENTION

You must check to ensure that the backup was completed with no errors before you can assume that the backup is usable. Check the Alarm Monitor for errors.

**ATTENTION**

You can schedule backups to run online while calls are being serviced. (Restores are performed offline.) However, because backups compete with services for system resources, schedule backups to run during off-peak hours. To determine the peak call processing periods, see [Chapter 2, “Configuring operational measurements,”](#) for more information.

Do not schedule backups during the MMFS audit hour (3:00 a.m. to 4:00 a.m., server time); they will not start while the MMFS audit is in progress.



## Opening the Backup Scheduler

### Introduction

View the schedule for a description of a scheduled backup from the Backup Scheduler. This window also lets you access the Event Properties window in which you schedule predefined backups.

### Administrative privileges required

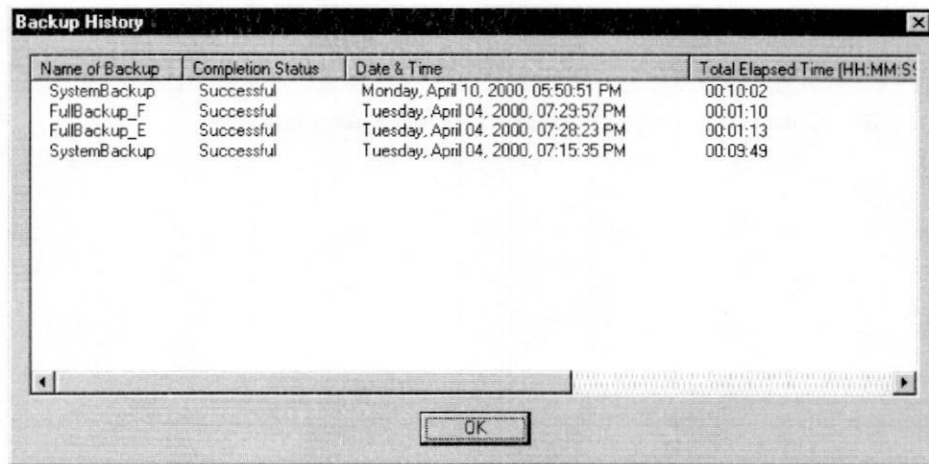
Log on as an administrator.

**Getting there** CallPilot System > System Administration > Server Backup > Backup Scheduler

### To open the Backup Scheduler

- 1 From Server Backup, double-click Backup Scheduler.

**Result:** The Backup History dialog box appears.



- 2 Use the left and right scroll bars to display additional columns showing
  - total size of the backup in kilobytes

- the name of the destination device
- the Primary (CallPilot) error code
- the Extended (Windows) error code

(See the *CallPilot Maintenance and Diagnostic Guide* for a complete list of CallPilot and Windows error codes.)

The table below gives brief descriptions of the more common error codes.

| Primary error  | Secondary error | Explanation                                                                                       |
|----------------|-----------------|---------------------------------------------------------------------------------------------------|
| 41807          | 1112            | There is no tape in the tape drive.                                                               |
| 41808          | 19              | The tape in the drive is write-protected.                                                         |
| 41825 or 41829 | 0               | The tape is blank or in a foreign format – use AutoFormat.                                        |
| 41827          | 1               | The incorrect tape driver is installed, or the tape medium is not compatible with the tape drive. |
| 41827          | 23              | Received a CRC error reading or writing – clean the drive or use a fresh tape.                    |
| 41828          | 1100            | The backup did not fit onto the tape – use a fresh tape or specify overwrite.                     |

- 3 Click OK to close the Backup History dialog box.

## Scheduling server backups

### Introduction

When you schedule a backup, it appears in the Backup Scheduler. To schedule a backup, open the Backup Scheduler to gain access to the Event Properties window.

#### ATTENTION

Backups compete with services for system resources. Schedule backups to run during off-peak periods and outside MMFS audit hours (3:00 a.m. to 4:00 a.m., server time).

### Before you begin

Ensure that the destination device to which the backup is performed is listed in the Backup Devices window. See [“Adding backup devices to the Backup Devices window”](#) on page 154.

#### Types of backups

The following server backup types are available:

| Backup type  | Description                                    |
|--------------|------------------------------------------------|
| SystemBackup | performs a backup of the system drives C and D |
| FullBackup_E | performs a backup of the secondary drive E     |
| FullBackup_F | performs a backup of the secondary drive F     |

**Autoformatting tapes**

All backup tapes must be specially formatted for CallPilot server backup data. When you schedule a backup, select Autoformat to format the tape immediately before the scheduled backup runs. This process destroys existing data on the tape the first time you autoformat for CallPilot.

The system can detect when a tape is already formatted for CallPilot, and it does not autoformat again.

**Overwriting existing data**

When you schedule a backup, select Overwrite to replace the contents of the tape with the new backup. If you do not select Overwrite, the new backup appends to existing backup data on the tape.

**Note:** If you schedule your system backup and your secondary disk backups at different times, but intend to use the same tape, do not select Overwrite on the second backup, or you overwrite the data from your first backup.

**Getting there** CallPilot System > System Administration > Server Backup > Backup Scheduler

## To schedule a backup

- 1 From the Backup Scheduler, click File > New Schedule.

**Result:** The Event Properties window appears.

**Event Properties** [?] [X]

General | Schedule | Others

Event ID: 951277513 Host Name: CPI0001

**Ownership**

Tag: Backup\_NGen

Owner: sysadmin

Customer ID: 1

**Main**

Device Name: PrimaryServerTape

Backup Definition: FullBackup\_E

**Submission**

Date: February 22, 2000

Time: 10:45:13 PM

**Additional options**

☐ Autoformat

☐ Overwrite

Save Cancel Help

- 2 Select the destination device in the Device Name box.
- 3 Select the type of backup in the Backup Definition box.
- 4 Select Autoformat to format the tape for CallPilot automatically before the scheduled backup runs.

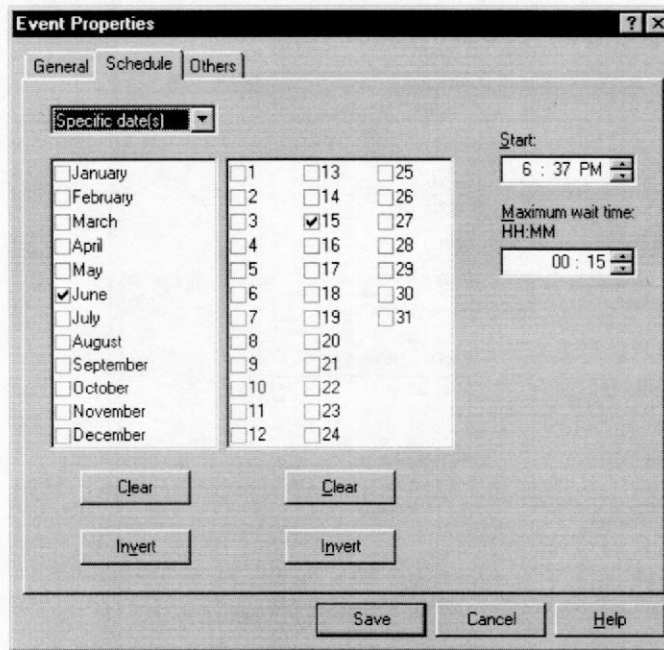
**Note:** You cannot perform a successful backup on an unformatted tape.

- 5 Select Overwrite if you want the backup to overwrite existing data on the device.

**Note:** If you are scheduling backups to run one after the other, and you intend to use the same tape, select Overwrite only on the first backup. If you select Overwrite on the subsequent backup, you overwrite the data from the first one.

- 6 Click the Schedule tab.

**Result:** The Schedule tab appears.



- 7 Select the day or dates on which the backup is going to run.

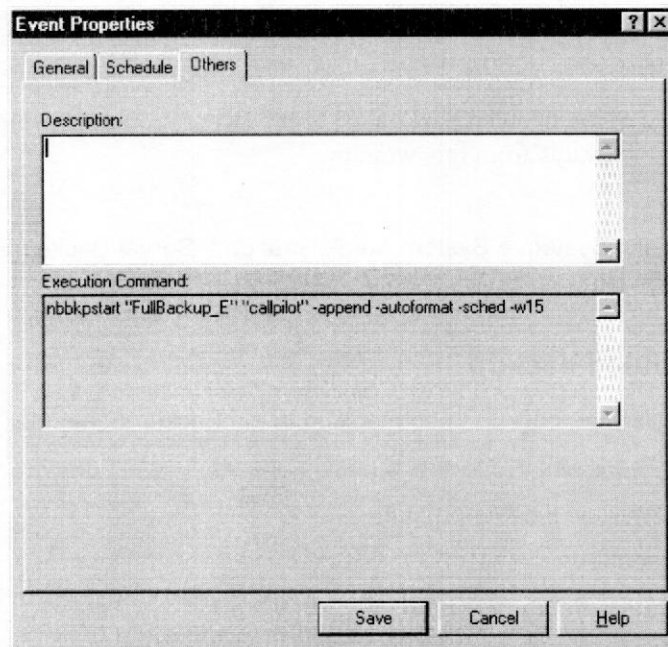
**Tip:** Click the drop-down arrow to access daily, weekly, monthly, yearly, or specific dates schedule selections.

- 8 Select the time for the backup to run.
- 9 Select the maximum wait time.



- 10 Click the Others tab.

**Result:** The Others tab appears.



- 11 Enter any explanatory details about the backup.  
12 Click Save.

**Result:** The system schedules the backup and adds it to the Backup Scheduler.

## Modifying and deleting scheduled backups

### Introduction

Modify details of a scheduled backup using the Event Properties window. You can also delete backups from this window.

**Getting there** CallPilot System > System Administration > Server Backup > Backup Scheduler

### To modify a scheduled backup

- 1 Double-click the backup to be modified in the Backup Scheduler.

**Result:** The Event Properties window appears.

- 2 Modify details in the General tab.
- 3 Click Schedule.
- 4 Modify details in the Schedule tab.
- 5 Click Other.
- 6 Modify details in the Others tab.
- 7 Click Save.

**Result:** The system modifies the backup and the changes appear in Backup Scheduler.

### To delete a scheduled backup

- 1 From Backup Scheduler, select the scheduled backup you want to delete.
- 2 From the File menu, select Delete.

## Monitoring or canceling backups

### Introduction

Monitor the status of a running backup using the Backup Status window. This window appears on-screen when a scheduled backup runs.

### Current status

View the current status to see if any files were skipped or copied in error during the backup.

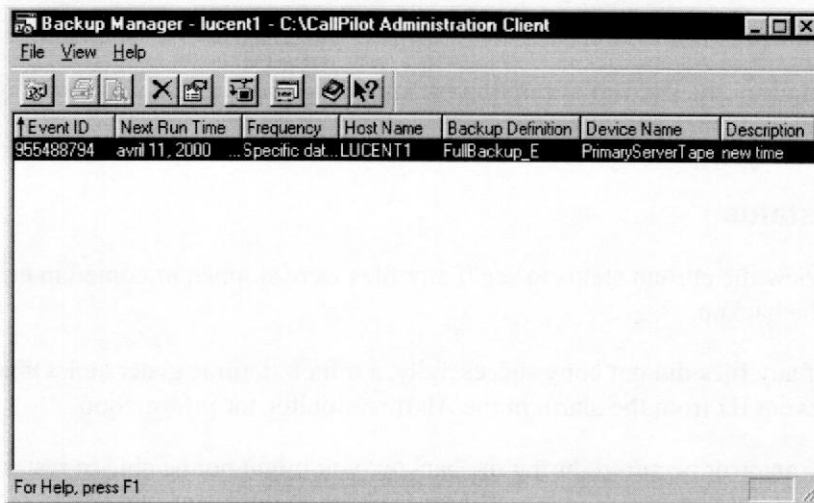
If any files did not copy successfully, a minor alarm is generated. Obtain the Event ID from the alarm in the Alarms Monitor for information.

If an error occurred during the backup, you might not be able to restore data from that backup medium. Repeat the backup until it has no errors.

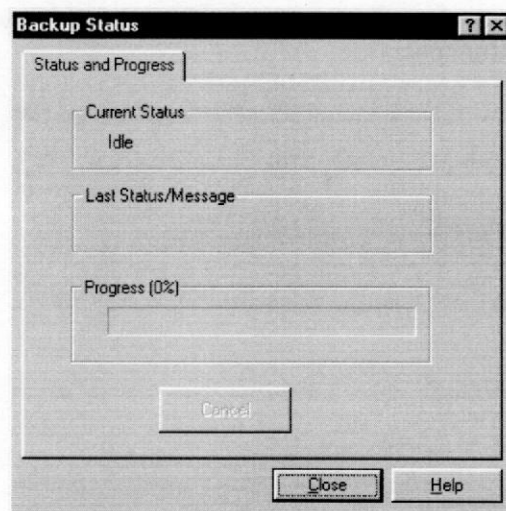
**Getting there** CallPilot Administration Client > System Administration > Server Backup > Backup Manager

## To view the current status

- 1 On the Backup Manager dialog box, click the current backup to highlight it, and then click View > View Backup Status.



**Result:** The Backup Status dialog box appears.



**To cancel a running backup**

Click Cancel on the Backup Status window to stop a running backup.

Any data that is successfully written to the backup device before the backup is canceled is unusable.

- The unusable data from the previous backup remains on the tape, and the data for the new backup is recorded following the unusable data.
- If a subsequent backup is appended to this tape, it is written to the tape following the unusable data.





## Section D: Setting up remote disk backups

### In this section

|                                                                     |            |
|---------------------------------------------------------------------|------------|
| <u>About remote disk backups</u>                                    | <u>176</u> |
| <u>Planning the configuration</u>                                   | <u>177</u> |
| <u>Creating a writable share on the remote file server</u>          | <u>179</u> |
| <u>Reconfiguring the backup and restore on the CallPilot server</u> | <u>199</u> |
| <u>Verifying the network configuration</u>                          | <u>204</u> |
| <u>Creating a disk device on the CallPilot server</u>               | <u>206</u> |

## About remote disk backups

### Introduction

You can configure the network to allow backups to be performed to a remote disk, such as a Windows 95/98 workstation or Windows NT server, rather than a tape drive.

To set up remote disk backup to other server types, contact the appropriate network administrator for assistance.

### Steps required

Complete the following steps to set up and perform remote disk backups to a suitable workstation or server:

1. Plan the configuration (on page [177](#)).
2. Create a writable share on the remote file server (on page [179](#)).
3. Reconfigure the Backup/Restore service on the CallPilot Server (on page [199](#)).
4. Verify the Network Configuration (on page [204](#)).
5. Create a Disk Device on the CallPilot Server (on page [206](#)).
6. Schedule a backup or archive to the Remote Disk Device (on page [159](#)).

## Planning the configuration

### Introduction

Before you can configure the network to allow backups to be performed to a remote disk, plan the configuration.

As part of the initial planning you must

- identify an appropriate workstation or file server to store your CallPilot backup
- ensure there is sufficient disk space on the target server to hold the planned backups
- determine the mode of security access and user verification that is required for the Backup and Restore service to access the remote disk backup directory

### Supported workstation or file server

The target workstation or file server for the remote disk backup must support long file names. Windows NT, Windows 95/98, and other servers that support file storage from a Windows PC are all acceptable.

### Required disk space

The target workstation or file server must have sufficient disk space available for the types of backups that are to be placed on the remote backup server.

To back up the entire system requires approximately 250 Mbytes, plus 10 Mbytes for each hour of storage on the system. For example, a 30-hour system requires 550 Mbytes of disk space to accommodate a backup of the entire system, while a 1000-hour system requires 10.25 Gbytes.

CallPilot selective archives can vary widely, depending on the number of items selected for the archive, but usually require much less disk space than a full set of system backups.

## Security and user verification

You must configure the target workstation or server so that the Backup/Restore service is granted access to the remote disk backup directory. The access control method you choose is determined by the configuration of the remote disk backup server and by the security requirements of your location.

There are two types of control methods, as follows:

- **Share-level access control** Allows access for all users. The backup directory is not password-protected.
- **User-level access control** Access is restricted to specific users. You must configure the backup/restore service as a user in the domain of the remote disk backup server.

If your remote disk backup directory is on a Windows 95/98 workstation, you can choose either share-level or user-level access control. On Windows NT remote disk backup servers, you must use user-level access control.

If your remote backup directory is on a FAT partition, you control access to the network share, since you cannot assign access permissions to the directory itself.

If your remote backup directory is on an NTFS partition, there is no need to control access to the network share. You can apply the permissions directly to the backup directory. This is preferable since it controls both local and remote access.

## Creating a writable share on the remote file server

### Introduction

Create a shared directory on the server that stores the CallPilot backup data. Do not use this directory for any other purpose. Regularly back up data to removable media using the site backup procedures in use at your location.

Based on the selected target network drive, set up the writable share as outlined in the appropriate procedure:

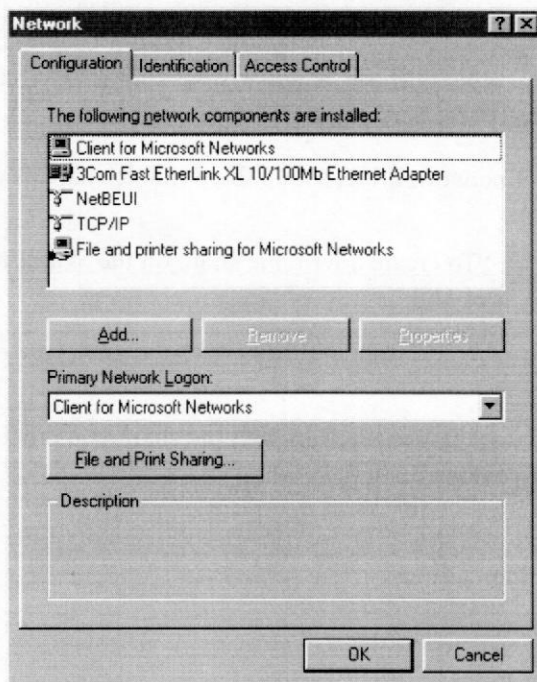
- For Windows 95/98, see "To create a writable share on the Windows 95/98 remote file server" on page 180.
- For Windows NT, see "To create a writable share on a Windows NT remote file server" on page 188.

**Note:** For Windows 95/98 workstations, ensure that the share you create is writable and *not* password-protected.

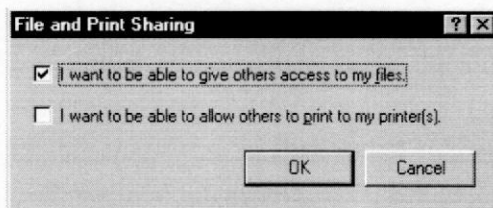


**To create a writable share on the Windows 95/98 remote file server**

- 1 Select Start > Settings > Control Panel.
- 2 Double-click Network to display the Network window.
- 3 On the Configuration tab, click File and Print Sharing... near the bottom of the window.



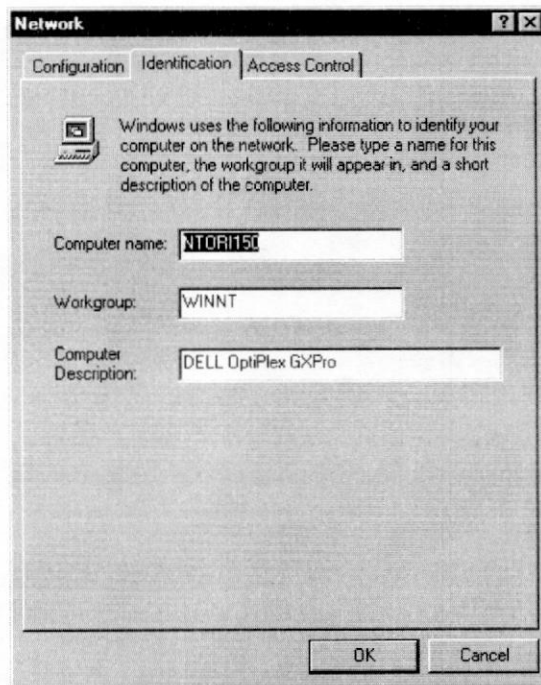
- 4 In the File and Print Sharing window, check the box labeled I want to be able to give others access to my files. This configures the computer to permit file sharing.



- 5 Click OK to exit the File and Print Sharing dialog box.



- 6 Select the Identification tab and note the Computer name assigned to this computer. You need this information when you set up the CallPilot server.

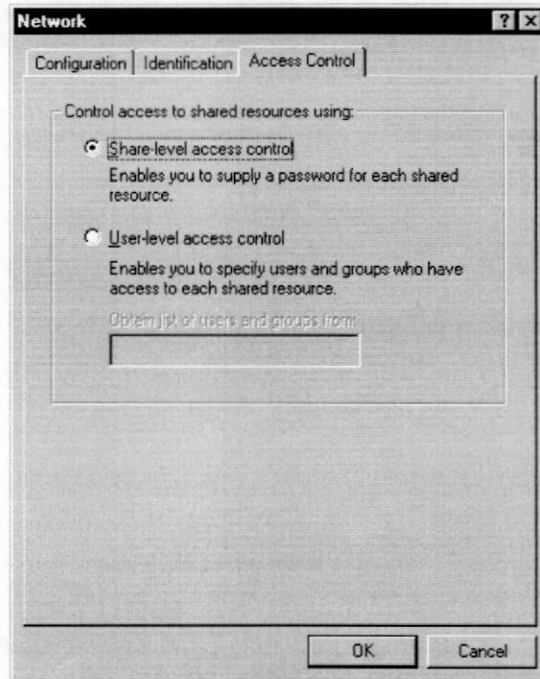


- 7 Determine the level of access to be assigned to the writable share, and proceed with the appropriate step, as outlined below:
- For Share-level access control, continue with step 8.
  - For User-level access control, continue with step 15.

**For Share-level access control:**

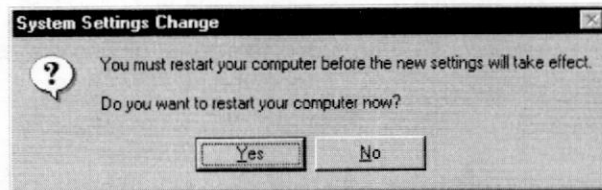
- 8 Select Share-level access control on the Access Control tab.

**Note:** Although Share-level access control is easier to set up, it is less secure than User-level access control.

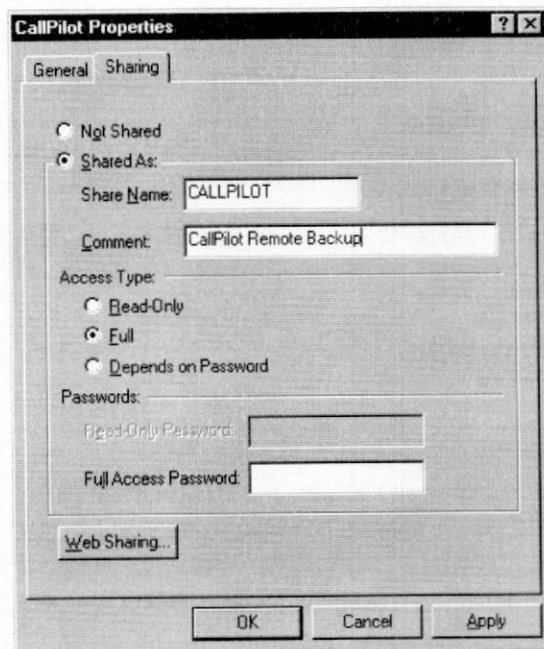


- 9 Click OK to exit the Network window.

- 10 If you have made changes, you are prompted to restart the computer. If you enabled file sharing, the system might require you to insert your Windows 95/98 CD so that some files can be copied to your system.



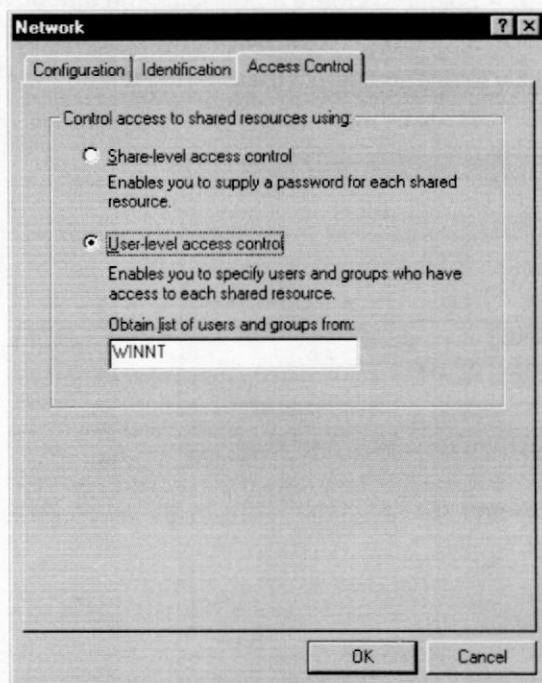
- 11 Click Yes to restart the computer and put the new setting into effect.
- 12 Create a shared directory for the remote disk backups, as follows:
- Open Windows Explorer and navigate to the drive you have chosen for remote disk backups. Highlight the drive name.
  - Select File > New > Folder to create a new folder on that drive (for example, D:\CallPilot Backups).
  - Right-click the new folder and select the Sharing tab on the Properties dialog box.



- d. Click Shared As, and type in a Share Name and optional comment. The share name must be 1 to 12 characters in length, using letters, digits, and underscore only. If you want to make this share invisible to workstation browsers, use a dollar sign as the last character.
  - e. Click Full from the Access Type group to assign full access permission to the remote backup directory. *Do not* type in a password.
- 13 Click OK to set the access permissions and create the share.
- 14 Refer to "What's next?" after step 23 to continue with the setup of the remote backup server.

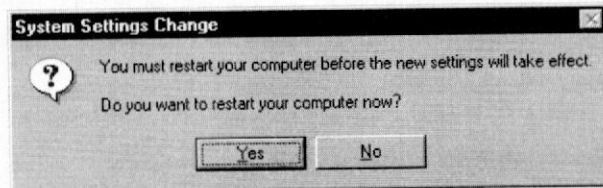
**For User-level access control:**

- 15 Select User-level access control on the Access Control tab. Make a note of the Windows NT domain from which you can obtain a list of users and groups.



- 16 Click OK to exit the Network window.

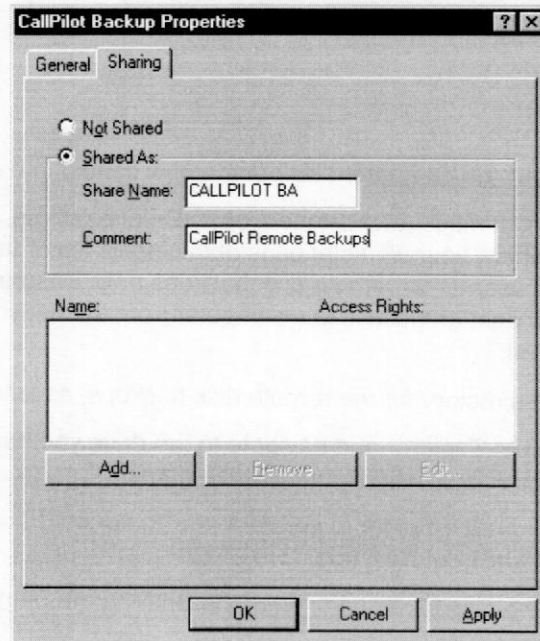
- 17 If you have made changes, you are prompted to restart the computer. If you enabled file sharing, the system might require you to insert your Windows 95/98 CD so that some files can be copied to your system.



- 18 Click Yes to restart the computer and put the new setting into effect.
- 19 Have the network administrator create a user ID (for example, CP\_Backup) on the domain where your workstation is obtaining its list of users and groups. Use this user ID for remote disk backups only. Ensure this user ID is set up with the right to "access this computer from the network." No other rights are required.
- 20 Create a shared directory for the remote disk backups, as follows:
- Open Windows Explorer and navigate to the drive you have chosen for remote disk backups. Highlight the drive name.
  - Select File > New > Folder to create a new folder on that drive (for example, D:\CallPilot Backups).
  - Right-click the new folder and select the Sharing tab on the Properties dialog box.



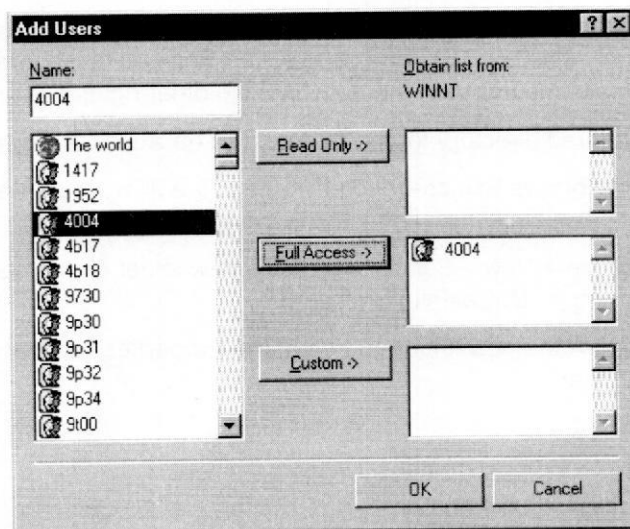
- d. On the Properties dialog box, select Shared As, and type in a Share Name and optional comment. The share name must be 1 to 12 characters in length, using letters, digits, and underscore only. If you want to make this share invisible to workstation browsers, use a dollar sign as the last character.



- 21 Assign user-level access permissions to the remote backup directory, as follows:
  - a. Click Add... on the Properties window to display the Add Users dialog box.
  - b. Select the user ID that you created in step 19 from the list on the left side.



- c. Click Full Access to move this user into the middle list on the right side.



- 22 Click OK on the Add Users dialog box to set the access permissions.
- 23 Click OK on the Properties dialog box to create the share.

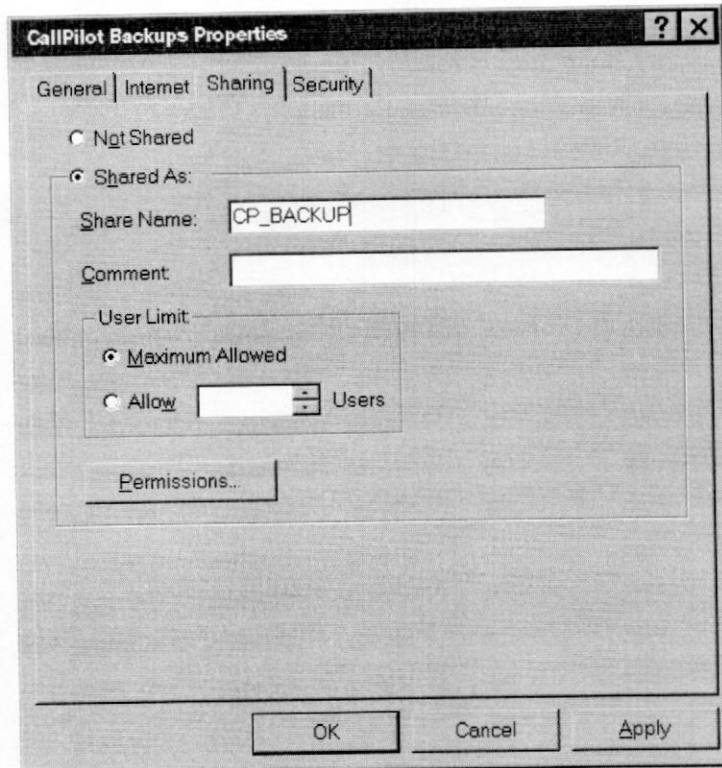
### What's next?

See [“Reconfiguring the backup and restore on the CallPilot server”](#) on page 199.

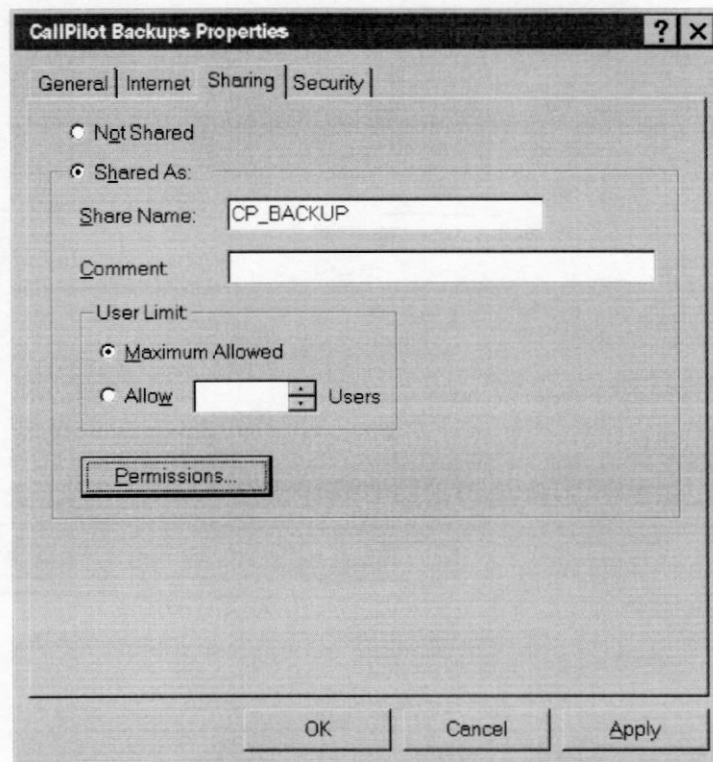
**To create a writable share on a Windows NT remote file server**

- 1 On your remote file server, create a local user to be used for remote disk backups only. This user ID (for example, CP\_Backup) must have the right to "access this computer from the network." No other rights are required.
- 2 Create a shared directory for the remote disk backups, as follows:
  - a. Open Windows Explorer and navigate to the drive you have chosen for remote disk backups. Highlight the drive name.
  - b. Select File > New > Folder to create a new folder on the selected drive (for example, D:\CallPilot Backups).
  - c. Right-click the new folder and open the Properties window. Select the Sharing tab.

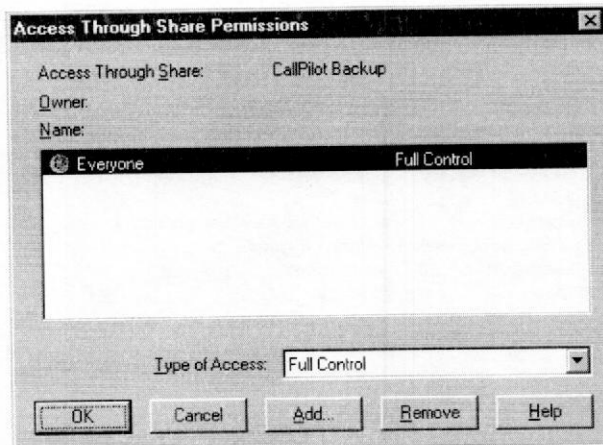
- d. On the Sharing tab, click Shared As, type a name in the Share Name box, and enter a comment in the optional Comment box. The share name must be 1 to 12 characters in length, using letters, digits, and underscore only. If you want to make this share invisible to workstation browsers, use a dollar sign as the last character.



- 3 Determine whether the remote directory is on a FAT partition or NTFS partition, and proceed with the appropriate step, as outlined below:
  - For FAT partitions, continue with step 4.
  - For NTFS partitions, continue with step 5.
- 4 For FAT partitions, assign access permissions to the remote backup directory share, as follows:
  - a. On the Sharing tab, click Permissions to assign access permissions to this share.

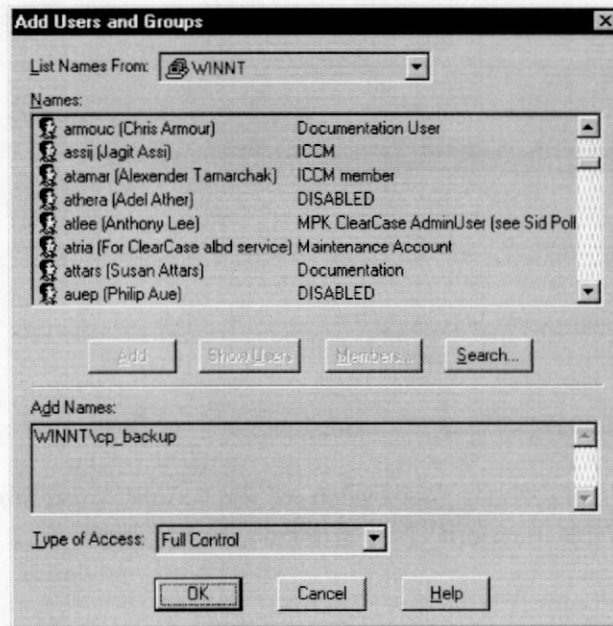


- b. On the Access Through Share Permissions dialog box, select Everyone and click Remove.



- c. Click Add to display the Add Users and Groups dialog box to add specific permissions.

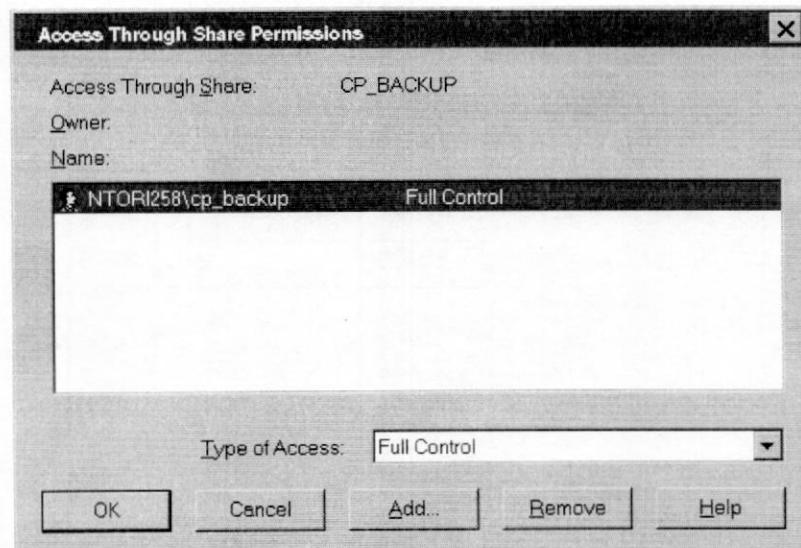
- d. On the Add Users and Groups dialog box, click Show Users, and select the user ID you created in step 1 from the Names list.



- e. Click Add to move this user into the Add Names text box.
- f. Select Full Control from the Type of Access combo box at the bottom of the window, and click OK.

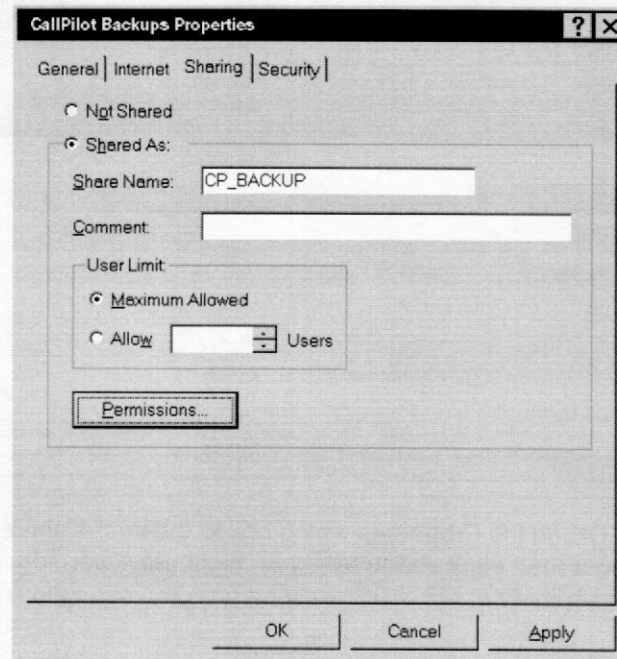


- g. On the Access Through Share Permissions dialog box, verify that the new user ID appears with Full Control, and then click OK.

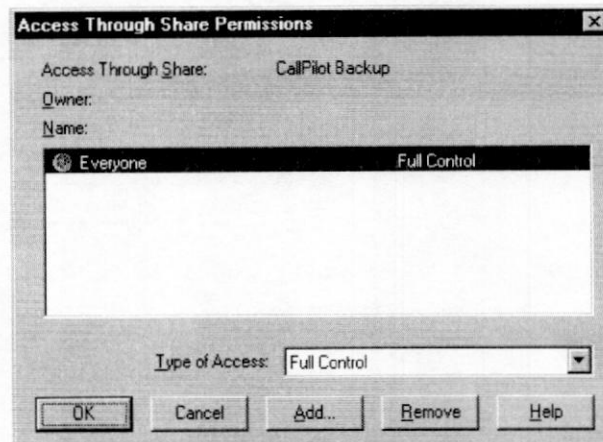


- h. Click OK on the Properties dialog box to create the share. If the name is longer than eight characters, you might get a warning about accessibility from MS-DOS workstations. You can ignore this warning.

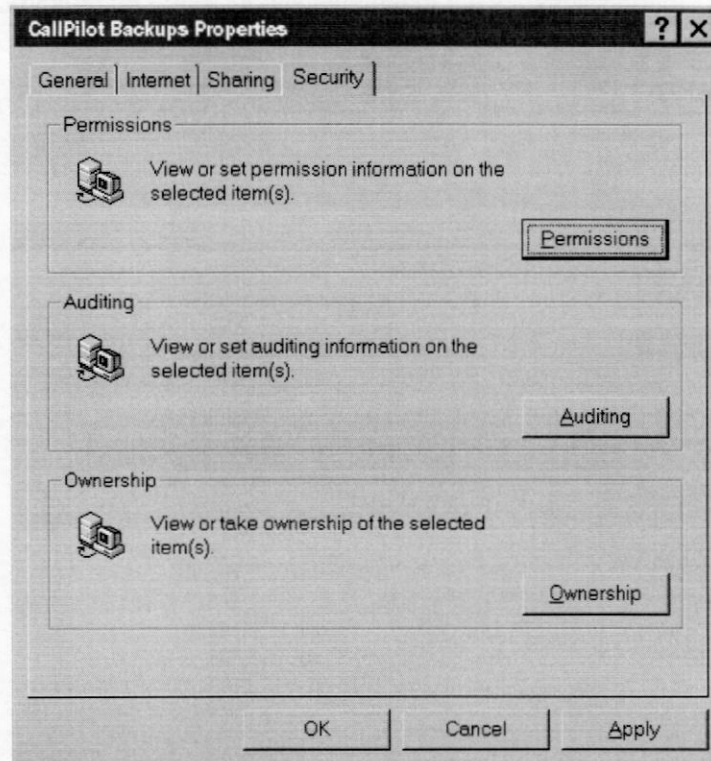
- 5 Assign access permissions to the remote backup directory NTFS partition, as follows:
  - a. On the CallPilot Backups Properties window, select the Sharing tab and click Permissions.



- b. On the Access Through Share Permissions dialog box, ensure the permissions are set to the default Everyone - Full Control.

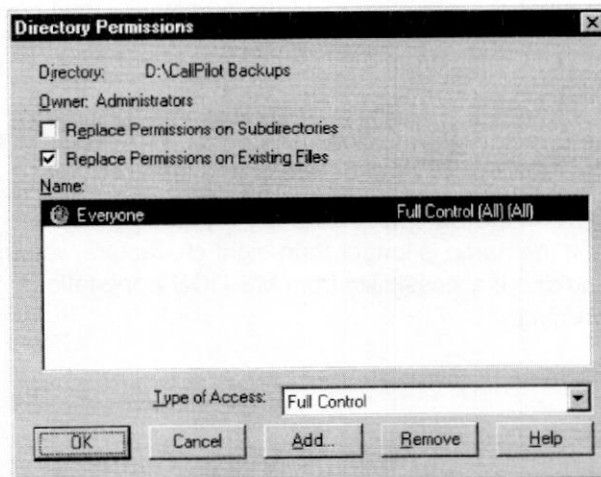


- c. On the CallPilot Backups Properties window, select the Security tab.

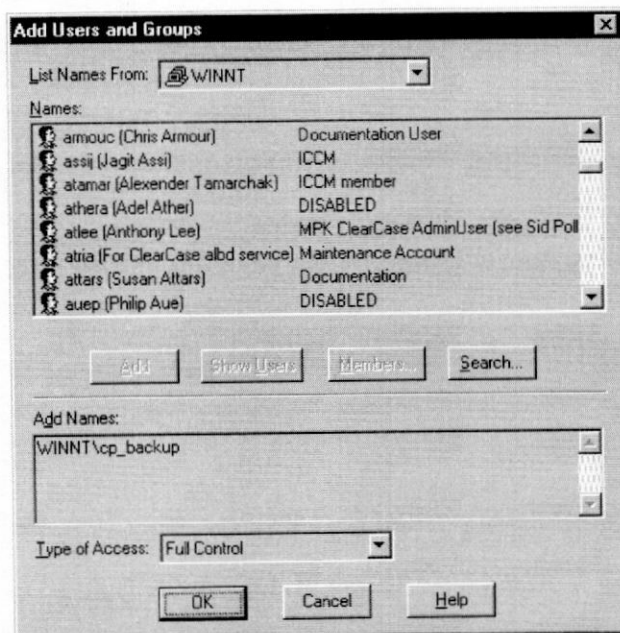


- d. Click Permissions to display the Directory Permissions dialog box. On the Directory Permissions dialog box, the default permissions are inherited from the parent directory.

- e. Select each item in the Name list box, and click Remove until the list box is empty.



- f. Click Add to display the Add Users and Groups dialog box to add specific permissions.





- g. On the Add Users and Groups dialog box, click Show Users, and select the user ID you created in step 1 from the Names list.
- h. Click Add to move this user into the Add Names text box.
- i. Select Full Control from the combo box at the bottom of the dialog box, and click OK.
- j. On the Directory Permissions dialog box, verify that the user ID appears with Full Control beside it, and then click OK.
- k. Click OK on the CallPilot Backups Properties window to create the share. If the name is longer than eight characters, you might get a warning about accessibility from MS-DOS workstations. You can ignore this warning.

### What's next?

See [“Reconfiguring the backup and restore on the CallPilot server”](#) on page 199.



## Reconfiguring the backup and restore on the CallPilot server

### Introduction

Once you have set up the shared directory on the remote backup server and assigned the appropriate network access permissions, configure the CallPilot server to access that shared directory.

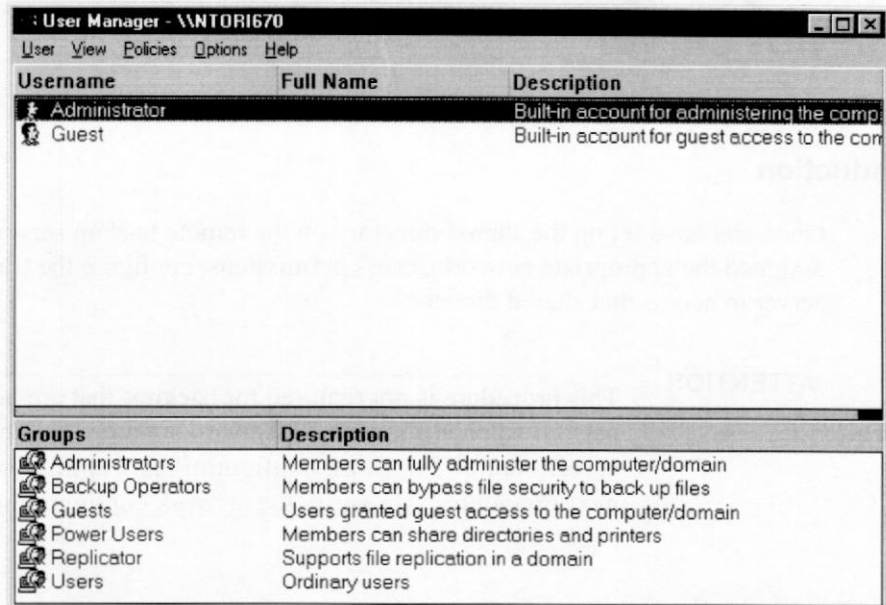
#### ATTENTION

This procedure is not required for backups that are being performed on a Windows 95/98 workstation using share-level access control. For those configurations, continue with the next procedure, "To verify the network configuration" on page 204.

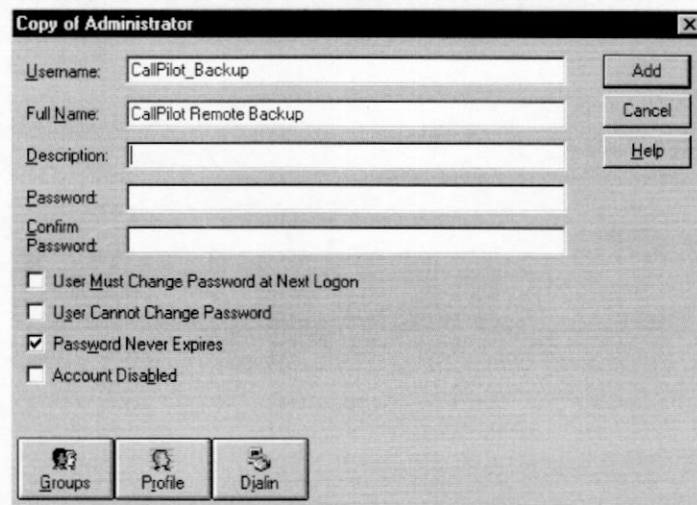
### To reconfigure the backup and restore on the CallPilot server

- 1 Log on to the CallPilot server using a user ID with administrative access.
- 2 From the Start menu, select Programs > Administrative Tools (Common) > User Manager for Domains.

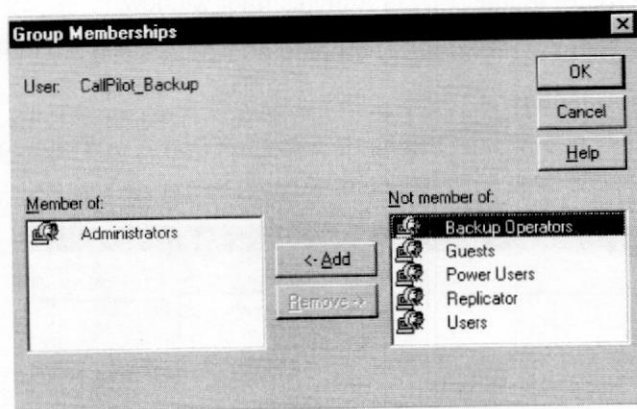
- 3 In User Manager, select the Administrator user ID from the list.



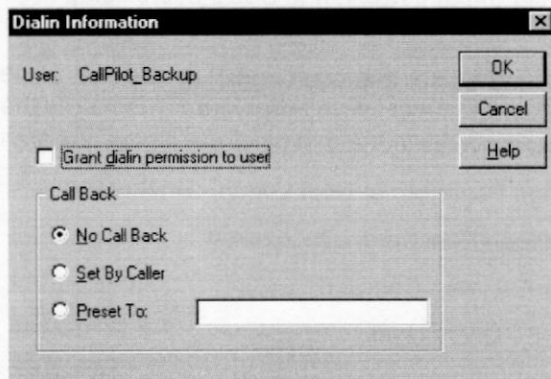
- 4 Select User > Copy from the menu bar. The Copy of Administrator dialog box appears.



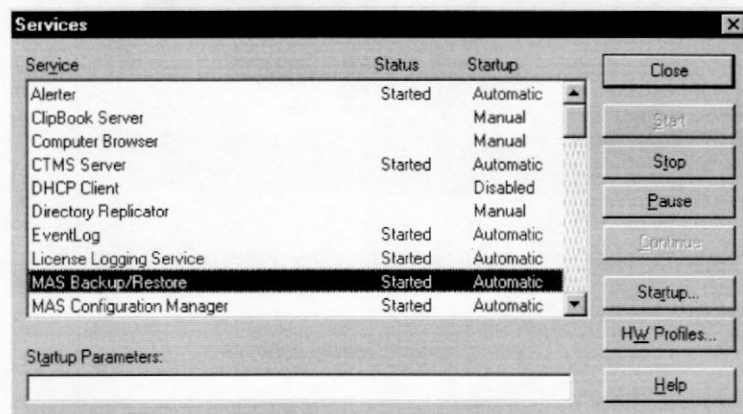
- 5 On the Copy of Administrator dialog box, in the Username field, enter the user name you created on the remote network domain for performing remote backups. Enter the Full Name and Description, using any characters that you want.
- 6 Enter the password for the user that you created for the remote network domain into the Password and Confirm Password fields. Verify that the settings for the following fields in the middle of the dialog box are correct:
  - User Must Change Password at Next Logon - Unchecked
  - User Cannot Change Password - Unchecked
  - Password Never Expires - Checked
  - Account Disabled - Unchecked
- 7 On the Copy of Administrator dialog box, click Groups, and verify that the new user is a member of the Administrators group.



- 8 On the Copy of Administrator dialog box, click Dialin, and verify that the new user does not have dial-in access.

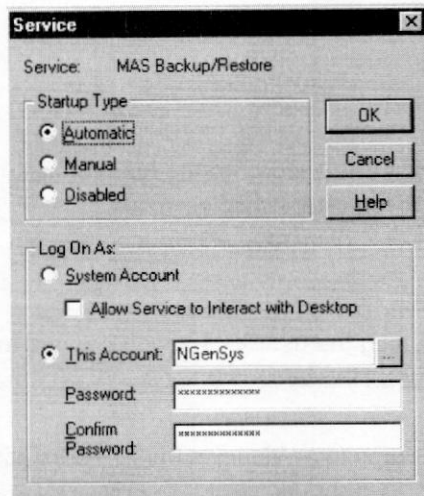


- 9 Click OK to return to the Copy of Administrator window.
- 10 Click Add to add the new user. The name now appears in the main list.
- 11 Exit the User Manager.
- 12 From the Start Menu, select Settings > Control Panel, and launch the Services applet.



- 13 Select the Backup/Restore service and click Start.vp

- 14 In the Log On As frame, select This Account.



- 15 Type in the user ID and password for the user you just created, and then click OK.
- 16 Stop, and then Start the Backup/Restore service on the Services window so that the new user ID and password settings take effect.
- 17 Close the Services applet and the Control Panel.

### What's next?

Verify the network configuration.



## Verifying the network configuration

### Introduction

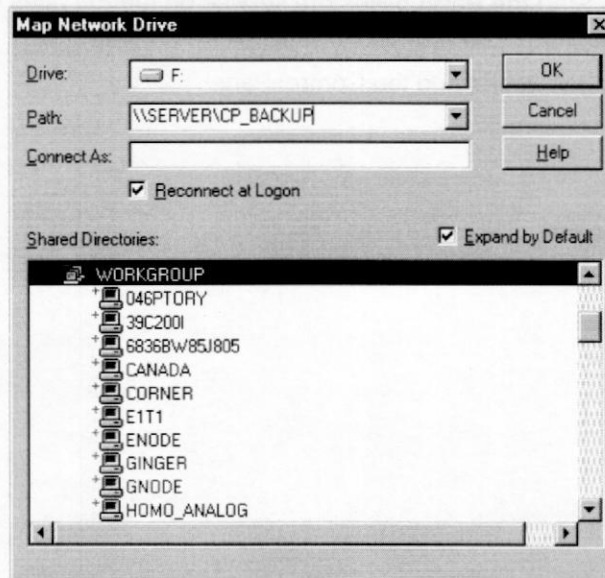
Verify the network access from the CallPilot server to the remote backup server to ensure that the remote access has been established correctly.

### To verify the network configuration

- 1 Log on to the CallPilot server, using the user ID that you created in the previous procedure, [“Reconfiguring the backup and restore on the CallPilot server”](#) on page 199.

**Note:** If you are performing backups to a Windows 95/98 workstation using share-level access control, log on as Administrator or any other server account known to you.

- 2 Open Windows Explorer and select Tools > Map Network Drive to display the Map Network Drive combo box.



- 3 Select an unused drive letter in the Drive combo box.



- 4 In the path combo box, type in the path to the remote backup directory. Use \\SERVER\CP\_BACKUP, where SERVER is the computer name of the remote backup server, and CP\_BACKUP is the share name of the directory you created.
- 5 Leave the Connect As text box blank, uncheck the Reconnect at Logon check box, and then click OK.  
**Note:** If you get an error message, verify that the computer name matches the remote file server's computer name exactly. Also, verify that the share name matches the remote file server's share name (not the directory name) exactly.
- 6 Try to copy a file into the root directory of the newly mapped drive.
- 7 Verify that the file has been created correctly, and that you can subsequently delete the file. If this cannot be done, verify the following information:
  - The user ID and password on the CallPilot server exactly match the user ID and password on the remote backup server's domain.
  - Full access permissions for the user ID have been assigned to the remote share or directory.
- 8 Select Tools > Disconnect Network Drive to delete the drive mapping you created.
- 9 Log off the CallPilot Server.

### What's next?

Create a disk device on the CallPilot server.

## Creating a disk device on the CallPilot server

### Introduction

Create a backup device that can be used to direct backups to the remote disk directory.

**Getting there** CallPilot System > System Administration > Server Backup > Backup Devices

### To create a disk device on the CallPilot Server

- 1 From the Backup Devices window, select File > New from the menu bar to create a new backup device.

**Result:** The New Backup Device Properties window appears.

- 2 In the Name field, enter a descriptive name.
- 3 In the Path field, enter the network path to the remote backup directory. For example, \\SERVER\CP\_BACKUP, where SERVER is the computer name of the remote backup server and CP\_BACKUP is the share name (not the directory name) of the shared directory that you created.

The name of the new backup device that was created in this step will appear in the dialog boxes that specify the name of the target device to which the backup or archive is directed.

**Note:** Do not use mapped drive letters to specify the path to the remote backup directory. These drive mappings are in effect only if a real user is logged on to the CallPilot server. If no user is logged on to the server, the drive mappings do not exist.

- 4 Click Save.

The CallPilot Administration Client can now be used to schedule backups or selective archives to the remote disk directory. See [Section C: "Scheduling server backups," on page 159](#) for information on scheduling system backups or archives.